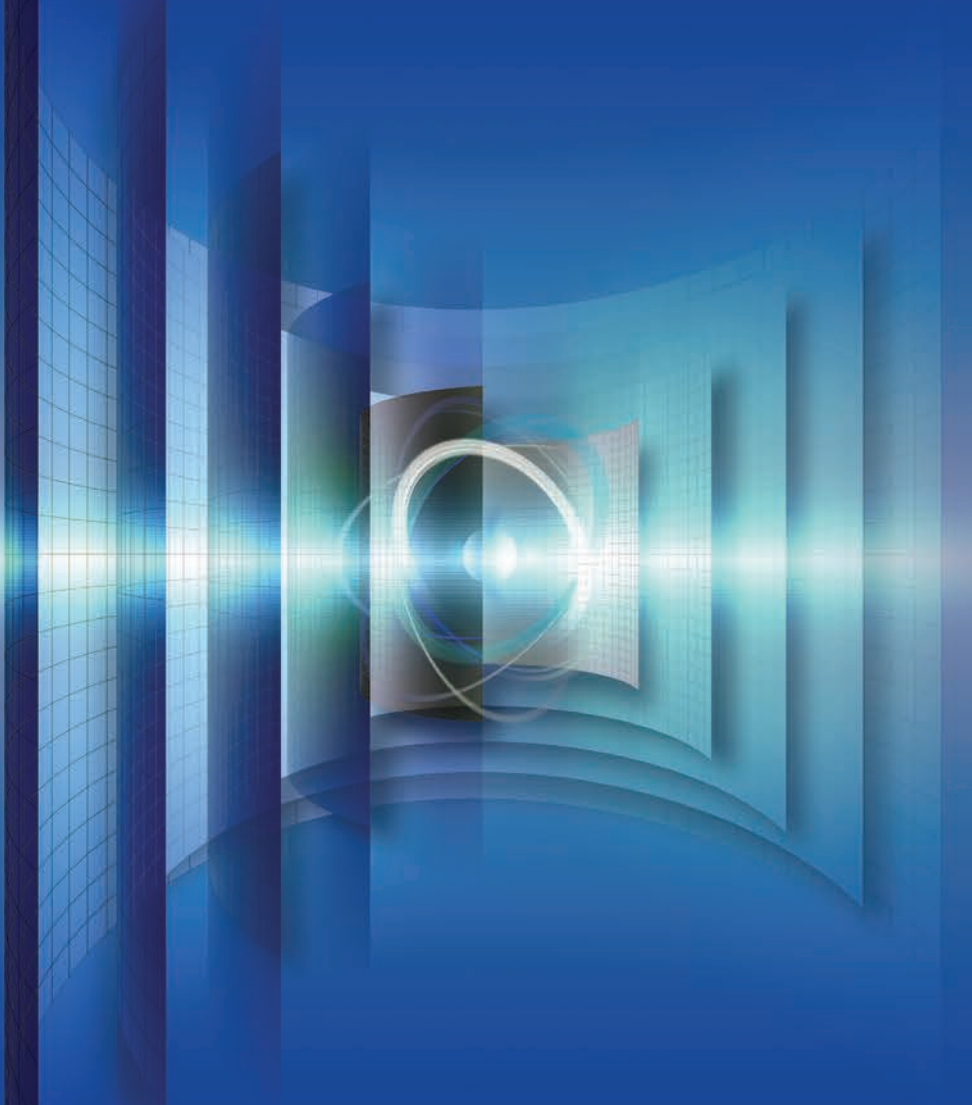
IAEA Nuclear Security Series No. 23-G

Implementing Guide

Security of Nuclear Information



IAEA
International Atomic Energy Agency

IAEA NUCLEAR SECURITY SERIES

Nuclear security issues relating to the prevention and detection of, and response to, criminal or intentional unauthorized acts involving, or directed at, nuclear material, other radioactive material, associated facilities or associated activities are addressed in the **IAEA Nuclear Security Series**. These publications are consistent with, and complement, international nuclear security instruments, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

CATEGORIES IN THE IAEA NUCLEAR SECURITY SERIES

Publications in the IAEA Nuclear Security Series are issued in the following categories:

- **Nuclear Security Fundamentals** specify the objective of a State's nuclear security regime and the essential elements of such a regime. They provide the basis for the Nuclear Security Recommendations.
- **Nuclear Security Recommendations** set out measures that States should take to achieve and maintain an effective national nuclear security regime consistent with the Nuclear Security Fundamentals.
- **Implementing Guides** provide guidance on the means by which States could implement the measures set out in the Nuclear Security Recommendations. As such, they focus on how to meet the recommendations relating to broad areas of nuclear security.
- **Technical Guidance** provides guidance on specific technical subjects to supplement the guidance set out in the Implementing Guides. They focus on details of how to implement the necessary measures.

DRAFTING AND REVIEW

The preparation and review of Nuclear Security Series publications involves the IAEA Secretariat, experts from Member States (who assist the Secretariat in drafting the publications) and the Nuclear Security Guidance Committee (NSGC), which reviews and approves draft publications. Where appropriate, open-ended technical meetings are also held during drafting to provide an opportunity for specialists from Member States and relevant international organizations to review and discuss the draft text. In addition, to ensure a high level of international review and consensus, the Secretariat submits the draft texts to all Member States for a period of 120 days for formal review.

For each publication, the Secretariat prepares the following, which the NSGC approves at successive stages in the preparation and review process:

- An outline and work plan describing the intended new or revised publication, its intended purpose, scope and content;
- A draft publication for submission to Member States for comment during the 120 day consultation period;
- A final draft publication taking account of Member States' comments.

The process for drafting and reviewing publications in the IAEA Nuclear Security Series takes account of confidentiality considerations and recognizes that nuclear security is inseparably linked with general and specific national security concerns.

An underlying consideration is that related IAEA safety standards and safeguards activities should be taken into account in the technical content of the publications. In particular, Nuclear Security Series publications addressing areas in which there are interfaces with safety — known as interface documents — are reviewed at each of the stages set out above by relevant Safety Standards Committees as well as by the NSGC.

SECURITY OF NUCLEAR INFORMATION

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GUATEMALA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA, ISLAMIC REPUBLIC OF
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world''.

IAEA NUCLEAR SECURITY SERIES No. 23-G

SECURITY OF NUCLEAR INFORMATION

IMPLEMENTING GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2015

COPYRIGHT NOTICE

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

Printed by the IAEA in Austria
February 2015
STI/PUB/1677

IAEA Library Cataloguing in Publication Data

Security of nuclear information. — Vienna : International Atomic Energy Agency, 2015.
p. ; 24 cm. — (IAEA nuclear security series, ISSN 1816–9317 ; no. 23-G)
STI/PUB/1677
ISBN 978–92–0–110614–8
Includes bibliographical references.

1. Nuclear industry — Security measures. 2. Nuclear facilities — Security measures. 3. Computer security. 4. Security systems. 5. Confidential communications — Access control. I. International Atomic Energy Agency. II. Series.

IAEAL 15–00954

FOREWORD

by Yukiya Amano
Director General

The IAEA's principal objective under its Statute is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." Our work involves both preventing the spread of nuclear weapons and ensuring that nuclear technology is made available for peaceful purposes in areas such as health and agriculture. It is essential that all nuclear and other radioactive materials, and the facilities at which they are held, are managed in a safe manner and properly protected against criminal or intentional unauthorized acts.

Nuclear security is the responsibility of each individual State, but international cooperation is vital to support States in establishing and maintaining effective nuclear security regimes. The central role of the IAEA in facilitating such cooperation and providing assistance to States is well recognized. The IAEA's role reflects its broad membership, its mandate, its unique expertise and its long experience of providing technical assistance and specialist, practical guidance to States.

Since 2006, the IAEA has issued Nuclear Security Series publications to help States to establish effective national nuclear security regimes. These publications complement international legal instruments on nuclear security, such as the Convention on the Physical Protection of Nuclear Material and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, United Nations Security Council resolutions 1373 and 1540, and the Code of Conduct on the Safety and Security of Radioactive Sources.

Guidance is developed with the active involvement of experts from IAEA Member States, which ensures that it reflects a consensus on good practices in nuclear security. The IAEA Nuclear Security Guidance Committee, established in March 2012 and made up of Member States' representatives, reviews and approves draft publications in the Nuclear Security Series as they are developed.

The IAEA will continue to work with its Member States to ensure that the benefits of peaceful nuclear technology are made available to improve the health, well-being and prosperity of people worldwide.

EDITORIAL NOTE

Guidance issued in the IAEA Nuclear Security Series is not binding on States, but States may use the guidance to assist them in meeting their obligations under international legal instruments and in discharging their responsibility for nuclear security within the State. Guidance expressed as 'should' statements is intended to present international good practices and to indicate an international consensus that it is necessary for States to take the measures recommended or equivalent alternative measures.

Security related terms are to be understood as defined in the publication in which they appear, or in the higher level guidance that the publication supports. Otherwise, words are used with their commonly understood meanings.

An appendix is considered to form an integral part of the publication. Material in an appendix has the same status as the body text. Annexes are used to provide practical examples or additional information or explanation. Annexes are not integral parts of the main text.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

BACKGROUND

1.1. The overall objective of a State's nuclear security regime is to protect persons, property, society and the environment from harmful consequences of a nuclear security event [1]. Groups or individuals wishing to plan or commit any malicious act involving nuclear material or other radioactive material or associated facilities may benefit from access to sensitive information. Such information should therefore be identified, classified and secured with the appropriate measures. Sensitive information is information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.

1.2. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes. Information security not only includes ensuring the confidentiality of information, but also includes ensuring the accuracy and completeness of the information (its integrity) and the accessibility or usability of the information on demand (its availability).

1.3. Ensuring the security of sensitive information is a cross-cutting prerequisite for nuclear security, and the systems and measures to achieve effective information security are key elements of a State's nuclear security regime.

1.4. The Nuclear Security Fundamentals [1] and all three Nuclear Security Recommendations publications [2–4] recognize the importance of securing sensitive information. This Implementing Guide expands on the high level statements in those publications to provide additional detail on what should be done.

OBJECTIVE

1.5. This publication provides guidance on implementing the principle of confidentiality and on the broader aspects of information security. Much national and international guidance exists regarding the establishment and management of information security frameworks for information of various types, in the form of both high level guidance and detailed standards. This publication does not intend to replace such guidance. Instead, its goal is to assist States in bridging the gap between existing government and industry standards

on information security in general, the particular concepts and considerations that apply to nuclear security, and the special provisions and conditions that exist when dealing with nuclear material and other radioactive material.

1.6. The objective of this publication is to provide guidance on:

(a) Establishing an effective framework for ensuring the confidentiality, integrity and availability of sensitive information (Section 3), including the necessary legislation and regulations;
(b) Identifying information that may be considered as sensitive information (Section 4);
(c) Considerations for the sharing and disclosure of sensitive information (Section 5);
(d) Guidelines and methodologies for ensuring confidentiality, integrity and availability (Section 6).

SCOPE

1.7. This publication addresses the security of sensitive information for civil uses of nuclear material and other radioactive material and associated facilities and activities. It focuses on sensitive information related to material and facilities that are under regulatory control.

1.8. Nuclear security as it relates to nuclear and other radioactive material out of regulatory control may also involve sensitive information that needs to be secured. In such cases, the general guidance provided here should be applied insofar as it is applicable.

1.9. The intended audience for this publication is anyone with a responsibility for the security of sensitive information. This includes:

(a) Competent authorities, including regulatory bodies;
(b) Management in facilities, companies and organizations involved in the use, storage or transport of nuclear material or other radioactive material;
(c) Facility operators and their staff, particularly the security staff;
(d) Contractors or other third parties working for the authorities, organizations or facility operators;
(e) Any other entities that may have been given legitimate access to sensitive information.

STRUCTURE

1.10. Following this introduction, Section 2 introduces several key terms and concepts that will be used throughout the publication. Section 3 describes the necessary elements that together build a framework for the security of sensitive information within a State, and Sections 4–6 address these elements in turn. Section 4 presents considerations for determining which information is sensitive information and therefore needs to be secured. Section 5 contains considerations for the sharing and disclosure of sensitive information. Section 6 describes in more detail the necessary actions at the facility level for securing sensitive information. Annex I provides an example of a classification framework. Annex II provides an example of a security categorization scheme for nuclear security related information. A suggested format and content of a training and awareness programme is given in Annex III.

2. CONCEPTS AND CONTEXT

2.1. This section clarifies the meaning of certain important terms as used in this publication. The section also applies the key concepts of information security to the context of nuclear security. Definitions of a wider range of relevant terms are provided in the Glossary, at the end of this publication.

INFORMATION

2.2. Information is knowledge, irrespective of its form of existence or expression. It includes ideas, concepts, events, processes, thoughts, facts and patterns. Information can be recorded on material such as paper, film, magnetic or optical media, or held in electronic systems. Information can be represented and communicated by almost any means. In the nuclear domain, there is a vast amount of information in many forms. Information assets are the equipment or components (including media) that are used to store, process, control or transmit information.

2.3. For the purpose of handling and security, information may be grouped into information objects. These may be defined as all elements of information that have value to an organization. Typically, an information object comprises

a set of data, information or knowledge that shares a common usage, purpose, associated risk or form of storage or transmission.

2.4. It is important to understand that nuclear security related information may have value (possibly of different natures and magnitudes) to any, or all, of the following:

(a) The State;
(b) Competent authorities;
(c) Facility operators (including third parties, such as vendors);
(d) A potential adversary (individuals and organized entities);
(e) The media;
(f) The public.

IDENTIFYING AND SECURING SENSITIVE INFORMATION

2.5. Sensitive information is information, the unauthorized disclosure (or modification, alteration, destruction or denial of use) of which could compromise nuclear security or otherwise assist in the carrying out of a malicious act against a nuclear facility, organization or transport. Such information may refer, for example, to the nuclear security arrangements at a facility, the systems, structures and components at a facility, the location and details of transport of nuclear material or other radioactive material, or details of an organization's personnel.

2.6. Identifying information that satisfies this definition is among the key steps in establishing an information security programme to ensure confidentiality. More detailed and comprehensive guidance on the topic is provided in Section 4, and illustrative examples are provided in Annex II.

2.7. Securing sensitive information is necessary because easy access to inadequately secured information can help adversaries to plan or commit malicious acts with relatively little effort or risk. If, for example, a facility's physical protection plan were acquired by adversaries planning an attack on the facility, they would know the obstacles they would face, the size and arming of the guard force, the size of the response force and the approximate time it would take for that force to arrive at the site. They would also know the important targets within the facility, their locations and the measures protecting them. Similarly, if an adversary wishing to steal nuclear material during transport succeeded in acquiring a device giving access to detailed information about the

planned transport — because the device had been inadequately secured — the adversary could plan an attack more effectively. Thus, the possession of such information or information assets by adversaries would increase the likelihood of their success.

2.8. Access to sensitive information and sensitive information objects should be no wider than is necessary for the conduct of an organization's business. By implication, the dissemination should be limited to those individuals who are appropriately authorized for access and only to those circumstances in which they need access. The 'need to know' and the 'need to hold' rules are fundamental to the security of sensitive information. These rules should guide the management and control of information access rights. The access rights should be reviewed periodically and when required.

2.9. Ensuring confidentiality depends on the application of security measures to selected sensitive information and sensitive information assets (the equipment or components, including media, that process, handle, store or transmit sensitive information) in order to ensure that it does not fall into the hands of unauthorized individuals or organizations, either external or internal. Guidance on measures against the insider threat is contained in Preventive and Protective Measures against Insider Threats [5]. Security measures should be based on risk analysis. The risk analysis should be kept up to date by a process of periodical reviews.

INFORMATION SECURITY

2.10. Information security, as described in this publication, refers to the system, programme or set of rules in place to ensure the confidentiality, integrity and availability of information in any form. At a minimum, it includes:

(a) Security of information in physical forms (e.g. paper and electronic media);
(b) Security of computer systems, sometimes referred to as computer security, information technology (IT) security or cybersecurity (additional IAEA guidance can be found in Computer Security at Nuclear Facilities [6]);
(c) Security of information assets (e.g. information storage and processing equipment, communication systems and networks);
(d) Security of information about facility employees and third parties (e.g. contractors and vendors) that could compromise the security of the above;
(e) Security of intangible information (e.g. knowledge).

2.11. While confidentiality is often singled out, organizations should ensure that their information security programme addresses all three attributes. Loss of integrity or availability can negatively affect nuclear security just as loss of confidentiality can. For example, if authorized users do not have timely access to information necessary for their duties (loss of availability), or if that information has been altered in such a manner as to mislead them (loss of integrity).

2.12. Information security should be considered and applied in the context of the overall security framework. It is closely interdependent with other security domains such as physical protection and personnel security. For example, physical protection measures can be used to protect sensitive information and sensitive information assets, while confidentiality measures make attack against physical protection systems more difficult or uncertain for adversaries. Gaps or shortfalls in any of the security domains can affect security in the others, so it is essential to use a comprehensive approach considering all domains together.

2.13. Information security should also consider the necessary balance between security and other objectives, including safety, openness and transparency, and operational aspects. Guidance on safety is provided in the IAEA Safety Standards Series.

3. FRAMEWORK FOR SECURING SENSITIVE INFORMATION

3.1. Securing sensitive information on a fragmented, facility by facility basis will not be effective. An effective national framework is necessary to ensure comprehensive security measures across all facilities, sites and organizations (governmental and non-governmental) handling sensitive information. The State should build this national framework, which will include establishing:

(a) The responsibility of the State;
(b) A legal and regulatory framework;
(c) National guidance;
(d) Security policies;
(e) Classification schemes.

Policies within each organization also contribute to the overall framework.

RESPONSIBILITIES

3.2. The responsibility for ensuring the existence and effective operation of a State's comprehensive nuclear security regime rests with the government of that State. Ensuring the security of sensitive information is an integral part of the nuclear security regime that the State should enforce.

3.3. States typically have government organizations or agencies that are responsible for overall national security, hereafter referred to as national security authorities. The national security authorities usually have the responsibility of defining the fundamental national policy on all aspects of security. The security policies and instructions issued by the national security authorities are often general in nature, and not specifically designed for nuclear security. However, many States' national security authorities do have policies and guidance for securing sensitive information, for example in government or military use.

3.4. The State's relevant competent authorities should develop and issue policy and requirements specific to the security of sensitive information at nuclear material and other radioactive material associated facilities and activities. These are usually based on, and in accordance with, any national security policy and requirements issued by the national security authorities, but taking into account the special nature of the activities that involve such materials. The competent authorities should also maintain close liaison with the national security authorities in order for the national threat assessment or design basis threat to be devised (for more information, see Development, Use and Maintenance of the Design Basis Threat [7]).

3.5. Each organization should establish its internal policy, plans and procedures for ensuring the confidentiality, integrity and availability of any sensitive information related to nuclear security that it holds or handles, and for protecting related sensitive information assets, in compliance with the national security policy and the relevant national laws and requirements. All employees should be fully aware of the need for information security and follow their organizations' information security rules and procedures.

LEGAL AND REGULATORY FRAMEWORK FOR SECURING SENSITIVE INFORMATION

3.6. Requirements for the maintenance of nuclear security within a State's boundaries should apply to all ministries, departments, agencies and

other organizations that deal with matters identified by the State to be necessary for national nuclear security. The State may impose these requirements by laws, regulations or other legally binding requirements. The State's requirements for nuclear security should include information security requirements. There should also be legislation in place that defines the sanctions or punishment that will be applied to any individual or organization who breaches such information security requirements. Such legislation may have sections which define the severity of particular types of breach of confidentiality or other information attributes and corresponding sanctions.

3.7. The competent authorities' regulatory powers should allow them to place obligations on the holders of sensitive information. The laws enacted for this purpose should mandate sanctions or punishment for unauthorized disclosure. The legislation should also mandate that State ministries, departments, agencies and other organizations provide the competent authorities with all necessary support to enable it to fulfil its task of ensuring the security of sensitive information.

PREPARING NATIONAL GUIDANCE

3.8. State policy on the security of information should define which type of information the State wishes to be secured and indicate how that security is to be applied. This is usually set out in a security manual compiled by the State's national security authorities (or other appropriate authority). A manual of this sort may not make any direct mention of sensitive information for nuclear security. The manual will, however, specify different classes of information indicating its level of sensitivity, and hence the level of security to be applied, and how information objects should be marked to ensure that the level of their sensitivity is obvious.

3.9. Detailed guidance on what constitutes sensitive information should be provided by the relevant competent authorities, in close liaison with the national security authorities and with the participation of users of nuclear material and other radioactive material. Such guidance is typically based on, and should be consistent with, the provisions of any national threat assessment. This type of guidance, sometimes referred to as classification policy, typically divides types of information into a series of related topics, and indicates the relative importance of a particular piece of information and thus its sensitivity and the degree of security to be applied.

3.10. At the organization level, the importance of particular information can be indicated in the organization's security plan, which should describe how particular sensitive information is to be protected in compliance with national legislation and regulations.

SECURITY POLICIES

3.11. In addition to issuing information security policies that comply with national requirements, the competent authorities should provide details of how these requirements should be applied to facilities and activities involving nuclear material and other radioactive material.

3.12. The State's policy on nuclear security should demonstrate a commitment to information security. It should encourage this through the issue and maintenance of a comprehensive and appropriate information security policy to be applied to all facilities and activities involving nuclear material and other radioactive material, as well as any other locations where related sensitive information is held. The aim of the policy is to ensure that sensitive information is secured against compromise.

3.13. Each organization and facility that handles sensitive information should then compile its own dedicated information security policy, based on that of the competent authorities where applicable. This policy should be communicated throughout the organization in a form that is relevant, accessible and understandable to the intended users. Section 6 contains additional guidance on establishing an information security management programme, including policies.

INFORMATION CLASSIFICATION SCHEMES

3.14. Implementing information security schemes and associated controls needs resources and time. It is not feasible or desirable to secure equally all information at a site or facility. Some information is non-sensitive and does not need any particular assurance measures. Even for sensitive information, different information objects may need different levels of security. It is therefore important to identify which information is sensitive information, and which level of security it requires. The competent authorities in each State should define which information concerning nuclear material, other radioactive material, associated facilities and activities constitutes sensitive information. Concerning

international transport, the State should identify which information needs to be secured and may want to consider consistency among the States involved in international transport.

3.15. The recommended way of assessing the value of a particular information asset is to use a risk informed approach, considering the damage and consequences that are likely to occur in the event of its compromise. It is important to note that any information compromise at one facility could affect other facilities with similar information assets; hence, the damage and consequences should be considered broadly for nuclear security effects at other locations and not just for one specific location. Specific consideration should be given to accumulations of information and potential single points of failure (e.g. information assets dependent on a single network or electricity supply). The results of this assessment could be used to determine the necessary level of security required for every information object, in accordance with the classification system used by the particular State.

3.16. A national system of classification should be established and maintained to group information into classes, such that the unauthorized disclosure of any of the information within a class would have similar consequences, and therefore that all information in a particular class should be subject to similar security requirements. This should be a national system, not specific to a particular industry or devised by a single facility. In many instances, States already maintain such classification systems, but such systems may not address nuclear security specific information. The system is based on a risk informed approach, where the potential consequences of unauthorized disclosure of information determine the class and the related security requirements for such information.

3.17. Careful consideration should be given to the number of classification categories and the benefits to be gained from their use. Very complex schemes may become cumbersome and prove impractical, whereas very simple schemes may not provide sufficiently precise classification. Furthermore, care should be taken when assigning a classification level to information objects. Overclassification (i.e. requiring more stringent security than is really necessary) can lead to unnecessary additional expense, whereas underclassification can put the information at an unacceptable risk of compromise. Overclassification may also conflict with policies on transparency or create a situation in which the classification becomes less meaningful to users of the information.

3.18. A possible classification scheme for sensitive information, with classes that indicate the sensitivity of particular information objects, might contain the following levels[1]:

(a) SECRET;
(b) CONFIDENTIAL;
(c) RESTRICTED.

3.19. Additional information labels may indicate the restrictions on distribution of the information arising from its classification, such as:

(a) No Further Distribution;
(b) Distribution Controlled by Originator;
(c) For Official Use;
(d) Restricted Distribution;
(e) Available for Public Use.

3.20. Example definitions for the classification levels SECRET to RESTRICTED are given in Annex I.

4. IDENTIFYING SENSITIVE INFORMATION

4.1. The first step in classifying and securing information is to identify the information that is considered sensitive information.

4.2. Security controls should be considered for information of at least the following types, which could affect nuclear security[2]:

(a) Details of physical protection systems and any other security measures in place for nuclear material, other radioactive material, associated facilities and activities, including information on guard and response forces;

---

[1] In many States, there is a further classification of TOP SECRET. This level of classification is almost never used in the civilian sector of most States. It generally applies in the military and weapons sector.

[2] This list is not meant to include all such possibilities, but it should provide a starting point for consideration.

(b) Information relating to the quantity and form of nuclear material or other radioactive material in use or storage, including nuclear material accounting information;
(c) Information relating to the quantity and form of nuclear material or other radioactive material in transport;
(d) Details of computer systems, including communication systems, that process, handle, store or transmit information that is directly or indirectly important to safety and security;
(e) Contingency and response plans for nuclear security events;
(f) Personal information about employees, vendors and contractors;
(g) Threat assessments and security alerting information;
(h) Details of sensitive technology;
(i) Details of vulnerabilities or weaknesses that relate to the above topics;
(j) Historical information on any of the above topics.

Some of the above information, such as personal information, may also be subject to specific security requirements under other national laws or company policies.

4.3. Annex II contains examples of specific types of information in the categories of para. 4.2, indicating whether they are typically considered to be sensitive information and why.

5. SHARING AND DISCLOSING SENSITIVE INFORMATION

5.1. There will often be a legitimate need to share sensitive information on an ongoing basis, for example among appropriate State agencies, among organizations handling nuclear material or other radioactive material and the relevant competent authorities, or among different States. Similarly, there will sometimes be a need to disclose sensitive information on an ad hoc basis to other organizations or the public. Both sharing and disclosure should be managed so as to ensure that sensitive information is not inadvertently shared with or disclosed to those who do not have a need to know.

SHARING INFORMATION

5.2. It is sometimes necessary for certain sensitive information to be shared with authorized State agencies or companies and organizations that have a need to know the information. Sharing information can create efficiencies that would not exist if the information were to be developed and handled independently. There are also occasions where not sharing information may damage security or weaken the overall planning, design and implementation of security measures. Furthermore, as nuclear security responsibilities are often not held exclusively by any single agency, company or organization, it is often necessary that information be shared among those who share the security responsibilities. For example, it is often necessary in the interests of national security for the competent authorities to pass sensitive information to the national security authorities and vice versa, for example changes in threat assessments or information on security events should be communicated in a timely fashion to relevant parties, in order to enable adjustment of security measures and exchange of operational experiences as a basis for continual improvement. In addition to security considerations, information sharing may be needed to support other objectives, including safety assessment, operational and commercial needs.

5.3. The nature and extent of sharing such information should be based firstly on compliance with national laws or regulations and then on a balance between the benefits obtained from sharing and the needs of security. Rules on the passing of information between such authorities should be governed by the security procedures that pertain in that State. Establishing a common approach within the State can ensure that sensitive information is not disclosed inappropriately.

5.4. It is often also necessary to share certain information with other States or relevant international organizations. In such a case, there should be an agreement in place to guarantee that sensitive information is secured by the recipient in a manner consistent with the requirements of the owner of the information. Security of information may be assured through a bilateral or multilateral treaty or agreement that defines how information will be secured against disclosure. Such agreements would typically describe the required protection measures to be applied to sensitive information for different classification levels in each State. They should also take into account how particular requirements in any one State (such as freedom of information legislation, see para. 5.6) might affect the handling of other States' sensitive information.

DISCLOSING INFORMATION

Need for disclosure

5.5. Most States have in place laws addressing the security of information of importance to the national interest. Such laws specify sanctions that will be imposed should a person, a national of that State or otherwise, breach the laws on confidentiality of such information. There are also usually laws that regulate an individual's access to official government information. There may be mechanisms to resolve disagreements between the government and other parties regarding which information can be withheld to protect national security.

5.6. Several States have freedom of information legislation or other laws that allow members of the public to request access to information held by the authorities. Typically, the only information that may be withheld by the authorities is that of types covered by specified exemptions, such as information associated with national defence, or private and personal information. In a number of States, an item bearing a classification marking is not automatically exempted from disclosure.

5.7. Other laws and regulations may require that certain types of information, which may include sensitive information, be disclosed. One example is environmental legislation that requires public reporting of specified information. It should be ensured that such laws allow exemption of information that might affect national security or the security of third parties.

Preparing guidance on disclosure

5.8. Specific guidance should be developed to assist organizations and facilities in deciding which sensitive information may be disclosed. When compiling such guidance, the responsible government agency will typically consult other government departments and relevant organizations. By identifying the type of information that it considers to be unsuitable for disclosure, the guidance should aim to prevent unauthorized disclosure of sensitive information (see also Annex II).

5.9. States should consider the need to provide specific guidance on:

(a) The sensitivity of certain types of sensitive information, based on the consequences of disclosure;

(b) Which types of information can be disclosed, under which circumstances, to whom and by which particular methods;
(c) Conditions on the disclosure of information;
(d) Processes to review information for its potential sensitivity prior to public presentation, such as in conference presentations, web postings or technical specifications;
(e) Which actions should be taken in any case of unauthorized disclosure of sensitive information, whether intentional or unintentional, or other breach of information security requirements.

5.10. The guidance will need to be subject to change. Circumstances evolve and information that might be considered sensitive and unsuitable for disclosure at one time might be significantly less sensitive and suitable for disclosure at a later time (or vice versa). Guidance should therefore be reviewed and updated periodically and in the event of significant changes in policy or circumstances.

5.11. Reducing the level of security applied to particular information, where appropriate, will generally be feasible. However, reclassification of information to a more restricted class may be impossible or ineffective if it has already been more widely disclosed. This should be taken into account in the original classification, and consideration should be given to the appropriate balance between confidentiality and caution, on the one hand, and availability and transparency, on the other. A default time frame for periodic review of classifications should be established, but changes should also be made when needed, for example if circumstances change significantly.

5.12. All requests to an organization for disclosure of sensitive information should be considered against the same guidance or criteria and, if possible, all such requests should be processed through a single central office for the organization. A technique commonly used to gain inappropriate access to sensitive information is to make multiple requests to different individuals or units within the same organization. If these requests are addressed separately, without coordination, different responses may be given and sensitive information may be disclosed that otherwise would not have been.

6. MANAGEMENT FRAMEWORK FOR CONFIDENTIALITY

6.1. Section 3 describes the high level framework for securing sensitive information. This section addresses in more detail the components of such a framework required within a facility or organization, placing them in the context of the management system.

6.2. A management system should be in place that establishes policies and objectives and enables the objectives to be achieved in an efficient and effective manner. An integrated management system (see IAEA Safety Standards Series No. GS-R-3, The Management System for Facilities and Activities [8], and associated guidance) is a vital support element to a nuclear security culture. Many activities at facilities are controlled by management systems. These ideally integrate security, safety, health, environmental, quality and economic elements in a single management process or a set of integrated and mutually reinforcing systems. Information security should be integrated into the existing management system of the facility or organization to ensure information confidentiality, integrity and availability.

6.3. Ensuring the confidentiality, integrity and availability of sensitive information depends on effective designation of roles and responsibilities, classification to identify which information is sensitive and needs to be secured, why it needs to be secured and to which level (see Section 4), decisions on how to secure such information, implementation of the necessary security measures, and response (including recovery) if such information is compromised, stolen or lost.

6.4. The management framework explained in the following applies to all levels of management at organizations holding or handling sensitive information.

RESPONSIBILITIES

6.5. Management has the overall responsibility for ensuring information security is in place and effective throughout the facility or organization, in order to secure sensitive information. All personnel who handle sensitive information have a responsibility to ensure its security in accordance with related national legislation as well as the organization's policies and procedures.

Management responsibilities

6.6. Management responsibilities typically include:

(a) Assuming overall responsibility for securing sensitive information and sensitive information assets;
(b) Ensuring compliance with relevant laws and regulations;
(c) Assigning organizational security responsibilities;
(d) Providing effective security training and education;
(e) Ensuring that an effective information security policy is established;
(f) Providing adequate resources to implement an effective information security programme;
(g) Ensuring development of the information security programme and associated plans and procedures;
(h) Ensuring effective change management related to plans, procedures and policies;
(i) Ensuring periodic audits, reviews and revisions of information security policy and procedures.

Classification responsibilities

6.7. Guidance on the classification to be applied to an information object should be provided by the relevant competent authorities in the form of a classification guide or guidance. Such a document groups information on particular topics and indicates the sensitivity of the information. Those who originate sensitive information should use such a guide when deciding on the appropriate classification level.

6.8. Once information has been disseminated, the recipient or holder of a sensitive information object should not change the classification level applied to the information without the permission of the originator. Recipients and holders of copies may, and when appropriate should, challenge the classification level applied. For example, if the competent authority received information from an operator that was incorrectly classified in reference to applicable laws, it should instruct the operator to change the classification.

6.9. In cases where the originating organization has ceased to function, its successor would become responsible. Where a successor cannot be traced, the holder of a sensitive information object may, if appropriate, change its classification level after consultation with the relevant competent authorities.

6.10. If the classification level applied to an information object or type of information objects is changed, the change should be notified as far as possible to everyone who might be affected. This may include current and past holders of the information, as well as those who might use it in future.

SECURITY PLAN

6.11. All organizations handling sensitive information should have a security plan. The security plan should have a detailed section dealing specifically with the security of sensitive information. The relevant requirements of the security plan should be communicated to employees and contractors working for the organization. It is essential that employees and contractors understand their responsibilities.

SECURITY POLICY AND PROCEDURES

Information security plan

6.12. Responsibility for information security should be included in an organization's hierarchy of policies and procedures. As a minimum, the following should be addressed:

(a) A definition of information security and a statement of its overall objectives, scope and importance.
(b) A definition of roles and responsibilities, including the establishment of a focal point to direct and manage information security.
(c) Compliance with information security requirements, including legal, regulatory and contractual requirements.
(d) The establishment of a risk management plan to reduce risks to an acceptable level, defined by the State, by applying adequate controls based on a risk assessment approach. For a nuclear facility, the risk management plan should be approved by the competent authority or other authority designated by the State.
(e) Regular monitoring and review of the arrangements in place to ensure that policy, standards and procedures remain relevant and effective.
(f) Requirements for education and training to ensure that staff, contractors and other personnel have an appropriate awareness of policy, procedures and practice to the extent necessary for their duties, and that they fully understand their responsibilities (including their legal obligations).

(g) The consequences (i.e. penalties or sanctions) for non-compliance with information security requirements or wilful negligence in securing sensitive information.
(h) Reference documentation that supports the policy, for example more detailed procedures for specific systems or security rules to which users should adhere.

Information security plan aspects specific to sensitive information

6.13. With specific reference to securing sensitive information, the plan should also cover:

(a) The information life cycle: definition of the processes to create, identify, classify, mark, handle, use, store, transmit, reclassify, reproduce and destroy sensitive information;
(b) The security requirements for sensitive information, giving due consideration to the security objectives of confidentiality, integrity and availability of the information;
(c) Restriction of access to sensitive information and sensitive information assets to those who need such access to perform their duties, who have the necessary authority and who have been subjected to a trustworthiness check commensurate with the classification level of the information;
(d) The transmission of sensitive information in a manner that reduces any risk of compromise, unauthorized interception, modification or disruption to an acceptable level.

Procedures for handling sensitive information

6.14. Effective management of risks from threats to the confidentiality, integrity and availability of information will involve developing effective countermeasures against such threats. This process will necessarily involve a combination of security controls drawn from information security, physical protection and personnel security.

6.15. Personnel security, including trustworthiness checks, ensures that those who have access to sensitive information are deemed by the State to be suitably trustworthy to do so. For information with a relatively low classification, the organization should decide whether any checks on those requiring access are needed; if so, a limited check of an individual's background may be sufficient. For access to information of higher classification, a more comprehensive set of background checks will be needed to determine trustworthiness. The personnel

security process should also include the execution of a non-disclosure agreement between the person and the competent authority or respective organization.

6.16. Physical protection often combines a degree of strictly managed access through a secure perimeter with one or more layers of other physical protection measures closer to the information assets, for example vaults and other secure locations. The same principles can be used to provide physical protection for information and information assets.

6.17. Information security measures include technical, procedural and administrative controls applied throughout the life cycle of information objects, including creation, handling, storage, transmission, replication and destruction. Information security measures include, among other things:

(a) Administrative management to govern, maintain and develop information security (including third party services);
(b) Personnel security, particularly in the phases of recruiting, and the beginning and end of employment;
(c) Physical security of areas where sensitive information or sensitive information assets are used, handled or located;
(d) Security of digital and manual information handling: workstation security, virus and malware protection, deletion and destruction of information, and manual processes;
(e) Communication network security (telephones, email, the Internet and local area networks): policy, user authentication, equipment identification, segregation, connection and routing controls, and monitoring;
(f) Equipment security: access control, logging of use, spare part management, backup of critical equipment, backup power arrangements, documentation and maintenance, cabling and media security;
(g) Software security: access control, logging of user and super user activities, backup management, maintenance contracting, configuration and version management, use of registered, legal software, testing for vulnerabilities and testing for system behaviour under error conditions;
(h) Security of use of information systems: user rights control, user recognition and verification, connecting to services, systems and equipment, password management, oversight of use, and the two person rule (i.e. two person control) for critical operations;
(i) Classification and corresponding procedures for handling information;
(j) Protection of privacy.

6.18. The handling of sensitive information should be governed by procedures in accordance with the information security section of national security policy and guidance, including any interpretation placed on it by the State's competent authorities. The minimum performance standards for various security levels should be described in the information security plan. An example would be the encryption methodology used for the electronic transmission of information.

Rights management system

6.19. A management system should be in place that establishes the control of how, why and when specific holders and users of sensitive information should be authorized to have access to the sensitive information and sensitive information assets. The rights management system typically includes:

(a) Defined structure of responsibility regarding authorization management;
(b) Defined processes about the function who has the right to appoint whom and who has the right to access sensitive information and sensitive information assets;
(c) Defined processes about how to verify, control and supervise the function of assigning access;
(d) Defined processes to determine how long an authorization to access sensitive information and sensitive information assets should last;
(e) Defined processes for revoking the authorization to access sensitive information and sensitive information assets;
(f) Defined processes to maintain full traceability of the management of rights in all steps of the management chain for the authorization to access sensitive information and sensitive information assets.

Periodic reviews

6.20. Security policies, plans and procedures should evolve according to changing circumstances. An effective way of ensuring that they are kept up to date may be to include a time frame for review in the policy document itself. Should there be a fundamental change in circumstances that might lead to a change in policy, for example a change in legislation, then a review may take place earlier. The review structure should apply to policy at all levels with nuclear security responsibilities.

SECURITY CULTURE

6.21. Developing, fostering and maintaining a robust nuclear security culture is an essential element of a nuclear security regime. This is especially true with information security in which people and processes are often the key factor in securing information.

6.22. As part of an effective nuclear security culture [9], all organizations, employees and contractors should have a full understanding of their security responsibilities and the importance of these responsibilities. It is essential that employees and contractors receive security education and training commensurate with their individual responsibilities and needs.

6.23. Employees and contractors with specific security responsibilities and those with access to sensitive information, as well as management at all levels of an organization, need specific training and briefings regarding their responsibilities. It is also important to ensure that other categories of employee (e.g. messengers, security personnel and clerks) who handle sensitive information without necessarily being aware of its content should also receive security training specific to their responsibilities.

6.24. One-off information security training events will not adequately reinforce training and may, over the long term, allow employees to become complacent. Everyone who handles sensitive information, including all management, employees and contractors, should receive continual on the job training and attend periodic refresher courses. Records of the formal training received and completed by all employees and contractors should be maintained. It is especially important that any changes in security rules and procedures should be made known to all relevant employees and contractors as soon as practicable. A suggested format and content of a training and awareness programme is given in Annex III.

INFORMATION SECURITY ARRANGEMENTS WITH THIRD PARTIES

6.25. A competent authority or an organization sometime needs a third party to provide services or goods that involve sensitive information. Such arrangements should be made through legal agreements such as a licence or contract, including non-disclosure agreements. Such agreements with third parties may involve sensitive information being put into the care of the third party. In order to ensure that such information is not put at risk, there should be a national policy or legislation covering arrangements in which sensitive

information is involved. Contracting organizations and facilities should then be obliged to follow that policy.

6.26. It is the responsibility of the contracting organizations when negotiating such relationships with third parties to ensure that any sensitive information entrusted to third parties is satisfactorily secured. Security measures in place to protect sensitive information should be commensurate with the risks and in accordance to the policy.

6.27. In this context, competent authorities and organizations should make certain that third parties:

(a) Have information security processes and procedures that meet at least the requirements of the organization's own security arrangements;
(b) Have a focal point to direct and manage security at the contracting company;
(c) Have in place a system to ensure that all staff with access to the sensitive information held by the third party have been subject to a trustworthiness check at an appropriate level;
(d) Ensure that access to sensitive information and sensitive information assets is limited to only those who have the necessary need to know and the appropriate security clearance;
(e) Transmit information in a manner compliant with national legislation, local policy and in such a way that information is not put at risk of compromise;
(f) Ensure that the information is not shared with any unauthorized party or individual;
(g) Ensure that all personnel have an appropriate awareness of security policy and practice and fully understand their responsibilities (including their legal obligations);
(h) Have procedures to address information security events;
(i) Ensure that security arrangements at the third party's premises are regularly inspected by the competent authorities or contracting organizations in accordance with the provisions of the agreement, to ensure that they are in compliance with the security requirements of the agreement.

INSPECTIONS AND AUDITS

6.28. Routinely performing assurance activities is essential to sustaining an information security programme. Assurance is needed that the security programmes in place at organizations holding sensitive information, including third parties, comply in all aspects with national policy and regulations. When

applicable, information security measures should be reviewed by the competent authorities before formal approval is granted for them to be used. Assurance may be achieved by regular, formal inspections or audits of the organization or facility. Audits are typically internal to the organization, whereas inspections can be performed both internally and externally. Additionally, inspections can be either announced or unannounced (i.e. with or without advance notice).

6.29. Internal inspections and audits are those carried out by the organization to determine whether the security programme in place complies with the approved information security plan and to ensure compliance with regulatory requirements. Such inspections allow an organization to check its own compliance at greater frequency than external inspections. Furthermore, inspections or audits conducted by personnel who are familiar with the internal requirements, procedures and systems may identify opportunities for improvement that differ from those an external inspection might discover.

6.30. External inspections are those conducted by the competent authorities or other authorized outside organizations. The aim of such inspections is to assess the level of compliance with a State's information security policy. External inspections provide an independent assessment, as compared with inspections conducted by the organization itself. When using external auditors, issues of confidentiality and trustworthiness should be addressed.

6.31. Inspection and audit results should highlight specific areas for action or improvement. Identified preventive and corrective actions should be assigned specific time frames for rectification or implementation. Rectification and implementation actions should be followed up and their effectiveness assessed.

INFORMATION SECURITY INCIDENTS

6.32. Breaches of security can result from the compromise of an information object. Two types of breach in which information is compromised are leaks and losses. Leaks are generally associated with a compromise of confidentiality where there has been an unauthorized disclosure, deliberate or accidental, of information. Losses are generally associated with a compromise of information resulting from theft of, or failure to appropriately secure, information or information assets.

6.33. Information security incidents may also involve loss of availability or integrity of information, which may be caused inadvertently or by intentional actions. Loss of availability may occur, for example, owing to a fault in an

information system (such as a database) or malicious denial of use (intentionally jamming an information network with excessive data traffic). Loss of integrity may be caused, for example, by damage to an information system, corruption of a database, or unauthorized alteration of information during transmission.

6.34. The reporting to the competent authorities of significant incidents or breaches of nuclear security, including information security breaches, should be mandatory, and this requirement should be embodied in a State's laws or regulations. The laws or regulations should also specify sanctions or penalties for failure to make such reports.

6.35. Heads of organizations and facilities should ensure that formal reporting arrangements are in place to ensure that all information security incidents are brought to their immediate attention so that corrective actions can be taken and, where appropriate, the incident reported to the competent authorities. Embarrassment should not be a reason for failing to report any information security incident at any level. Incidents should be reported promptly so that appropriate corrective action may be taken and trends may be identified.

INVESTIGATIONS

6.36. All information security incidents should be investigated. Policies and procedures should be defined governing information security incident investigation. An investigation should aim to determine whether a security incident has a minor or major impact on information security and confidentiality. The competent authorities may then initiate any appropriate action. An example of a minor incident may be a failure to lock up or secure a document properly that did not result in the loss or compromise of any information. A major incident, for example, may be the theft of a security plan that results in a strategic threat to an organization.

6.37. An investigation should:

(a) Look fully into the circumstances of the incident to establish the scope, scale and effect.
(b) Assess the consequences of the incident and the degree of compromise that may have occurred.
(c) Assess the need for further actions or wider enquiries, possibly to include other agencies.

(d) Recommend corrective actions or take action to contain or minimize the consequences.
(e) Report the outcome of the investigation, including:
    (i) The probable cause of the incident;
    (ii) The assessed degree of compromise;
    (iii) The likely effect(s) of the compromise;
    (iv) Possible recommendations on improvements to the security programme in order to avoid a similar incident;
    (v) Recommended further actions warranted by the incident;
    (vi) Lessons that need to be learned by the concerned parties.

6.38. The competent authorities should maintain records of the number and type of reported information security incidents. Recurring incidents or trends in security failures should be identified and may indicate the need for changes to security policy or improvements in security procedures or programmes. Updates on trends and changes should also be included in awareness training so that an appropriate security culture among employees and contractors is maintained. Organizations and facilities should also maintain their own records.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Objective and Essential Elements of a State's Nuclear Security Regime, IAEA Nuclear Security Series No. 20, IAEA, Vienna (2013).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Radioactive Material and Associated Facilities, IAEA Nuclear Security Series No. 14, IAEA, Vienna (2011).

[4] EUROPEAN POLICE OFFICE, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL CRIMINAL POLICE ORGANIZATION–INTERPOL, UNITED NATIONS INTERREGIONAL CRIME AND JUSTICE RESEARCH INSTITUTE, UNITED NATIONS OFFICE ON DRUGS AND CRIME, WORLD CUSTOMS ORGANIZATION, Nuclear Security Recommendations on Nuclear and Other Radioactive Material out of Regulatory Control, IAEA Nuclear Security Series No. 15, IAEA, Vienna (2011).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Development, Use and Maintenance of the Design Basis Threat, IAEA Nuclear Security Series No. 10, IAEA, Vienna (2009).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-R-3, IAEA, Vienna (2006).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Culture, IAEA Nuclear Security Series No. 7, IAEA, Vienna (2008).

Annex I

CLASSIFICATION SYSTEM AND DEFINITIONS

I–1. Annex I provides an example of a classification framework. Individual States may devise and use any appropriate classification system to indicate the level of sensitivity of nuclear security information. The definitions given in the following represent a four-level system similar to that of many Member States. The fourth level TOP SECRET is not discussed, as experience has shown that in the civil nuclear field it is very unlikely that any information assets would attract the classification TOP SECRET. Note also that while information is primarily envisioned as being in the form of documents or knowledge, items of equipment or other physical objects may be classified when classified information may be derived from them by visual observation of internal or external appearance, structure, operation, test, application or use.

SECRET

I–2. The compromise of information or material classified SECRET would be likely:

(a) To raise international tension;
(b) To cause serious damage to relations between governments;
(c) To threaten life directly, or seriously to prejudice public order, or individual security or liberty;
(d) To cause serious damage to the operational effectiveness or security of national security forces or the continuing effectiveness of highly valuable security or intelligence operations;
(e) To cause substantial material damage to national finances or economic and commercial interests;
(f) To be of use to an individual or group planning a malicious act which could cause grave damage at a facility with, or during transport of, nuclear material or other radioactive material.

CONFIDENTIAL

I–3. The compromise of information or material classified CONFIDENTIAL would be likely:

(a) To damage diplomatic relations;
(b) To prejudice individual security or liberty;
(c) To cause damage to the operational effectiveness or security of national security forces or the effectiveness of valuable security or intelligence operations;
(d) To work substantially against national finances or economic and commercial interests;
(e) To substantially undermine the financial viability of major organizations;
(f) To impede the investigation or to facilitate the commission of serious crimes;
(g) To impede seriously the development or operation of major government policies;
(h) To shut down or otherwise substantially disrupt significant national operations;
(i) To be of use to an individual or group planning a malicious act which could cause serious damage at a facility with, or during transport of, nuclear material or other radioactive material.

RESTRICTED

I–4. The compromise of information or material classified RESTRICTED would be likely:

(a) To affect diplomatic relations adversely;
(b) To cause substantial distress to individuals;
(c) To make it more difficult to maintain the operational effectiveness or security of national security forces;
(d) To cause financial loss or loss of earnings potential to, or to facilitate improper gain or advantage for, individuals or companies;
(e) To prejudice the investigation of crime;
(f) To facilitate the commission of crime;
(g) To breach proper undertakings to maintain the confidence of information provided by third parties;
(h) To impede the effective development or operation of government policies;
(i) To breach statutory restrictions on disclosure of information;

(j) To disadvantage government in commercial or policy negotiations with others;
(k) To undermine the proper management of the public sector and its operations;
(l) To be of use to an individual or group planning a malicious act which could cause significant damage at a facility with, or during transport of, nuclear material or other radioactive material.

I–5. With regard to applying the above classification levels to the control of nuclear sensitive information, consideration should be given to how the unauthorized disclosure of such information could assist a potential adversary in the following:

(a) Selecting a target for an act of theft, or sabotage of nuclear material or other radioactive material, equipment or facilities.
(b) Planning or committing an act of theft or sabotage of nuclear material or other radioactive material, equipment or facilities:
    (i) Design of security systems;
    (ii) Building plans;
    (iii) Methods and procedures for the transfer, accountability and handling of nuclear material or other radioactive material;
    (iv) Security plans, procedures and capabilities.
(c) Measuring the success of an act of theft or sabotage of nuclear material or other radioactive material, equipment or facilities:
    (i) Actual or hypothetical consequences of the sabotage of specific vital equipment or facilities.
(d) Illegally producing a nuclear explosive device, radiological dispersal device or radiation exposure device:
    (i) Design information useful in developing a device;
    (ii) Location of materials required to manufacture a device;
    (iii) Location of a nuclear weapon.
(e) Dispersing nuclear material or other radioactive material in the environment:
    (i) Location, form and quantity of materials.

Annex II

EXAMPLES OF SENSITIVE INFORMATION

II–1. Annex II provides an example of a security categorization scheme for nuclear security related information. The State should decide the exact level of classification to be applied to each item of such information. Table II–1 provides examples of sensitive information and identifies the sensitivity issues associated with them. Where release of the information is not recommended, the table suggests the reasons and whether security might be warranted.

II–2. The categories of information as presented in Table II–1 are only indicative of what might be considered sensitive information. They are not intended as a comprehensive list or model. The relevance of the categories to be considered for inclusion in any similar national table would be made according to a specific assessment by the State.

II–3. Within each row of the table, the first column describes an example type of information. The second column indicates whether this category is usually applicable to nuclear material and nuclear facilities (N), other radioactive material and associated facilities (R), or both (N, R). The third column gives an indication of whether the information might be considered sensitive or not sensitive. The final column provides some explanation of the sensitivity of the information and the rationale for securing it.

II–4. With regard to the designation of information as sensitive and the assignment of a potential classification level, consideration should be given to information that has already appeared in the public domain, or any previous compromise or possible compromise of information. It may be impractical to assign and manage a classification level for such information.

II–5. Consideration should also be given to designating non-sensitive information as sensitive if it, combined with other non-sensitive information, can be used to reveal sensitive information.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION

Category	Area	Sensitivity	Rationale for securing
1. SECURITY OF MATERIAL AND FACILITIES			
1.1. Regulations and guidance			
A. National security regulations governing the use of nuclear material or other radioactive material	N, R	Not sensitive	Such information is typically published in the public domain.
B. Guidance to such regulations, issued by the competent authority or other government agency	N, R	Sensitive	While not all such guidance may be sensitive, a document of this nature could contain details of standards, types of equipment to be used, procedures and security operations at a facility. Such details could be of use to adversaries planning a malicious act.
1.2. National nuclear security policies			
A. General government policies on matters involving nuclear material or other radioactive material	N, R	Not sensitive	Such information is typically in the public domain.
B. Detailed policy covering specific security topics	N, R	Sensitive	It might give an indication to the sort of obstacles adversaries may face, allowing them to plan the acquisition of more detailed information.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
1.3. Facility security plan	N, R	Sensitive	They typically contain detailed descriptions of the security measures in place at a site and precise detail of where within the site material is stored. For nuclear facilities, the plans also contain details of other areas essential to the operation of the site.
1.4. Security reports			
A. Reports from security surveys, inspections and assessments and other reports on the physical protection or technical security measures employed at a site or facility	N, R	Sensitive	Access to these reports may provide adversaries with detail on the location of material, the measures taken to protect it and any assessed vulnerabilities there may be, thus assisting them to avoid security measures and controls.
B. Reports describing critical features and/or highlighting requirements for security improvements, including at vital areas (if applicable)	N, R	Sensitive	Information of this nature could be of use to adversaries wishing to avoid security arrangements and could assist the targeting of a facility.
C. Results of security investigations at a site or facility, including those into leaks and losses of sensitive information	N, R	Sensitive	Information of this nature could be of use to adversaries wishing to avoid security arrangements and could assist the targeting of a facility.
D. Reports describing vulnerabilities of the security management system and consequences of failure	N, R	Sensitive	Information of this nature could be of use to adversaries wishing to bypass security arrangements.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
1.5. Construction details			
A. Details of construction and layout of locations in which material may be stored or processed, including drawings or plans held on any media, showing features of physical protection relevant to the prevention of malicious acts	N, R	Sensitive	Official maps, chart or plans of sites may be released at the discretion of site management, provided they contain no description of the details of a building's functions, the materials stored within, and the location of internal security fences and the other security measures employed at the building.
B. Details of construction of vital areas at nuclear power plants and other nuclear facilities	N	Sensitive	Information of this nature can help adversaries to avoid security arrangements and could possibly assist the targeting for sabotage purposes.
1.6. Protection systems			
A. Details of any physical protection measures in use, for example alarms, surveillance cameras, access controls, security personnel, etc.	N, R	Sensitive	
B. The types and locations of intrusion detection system sensors and the associated surveillance cameras, including circuit diagrams, location of critical power supplies, cable runs, the maintenance and testing programmes for this equipment	N, R	Sensitive	Any details of this nature would be of use to any adversary who wished to defeat the security systems at a facility.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
1.7. Details of automated access control systems, including the location of computer servers and backup servers and their power supplies	N, R	Sensitive	Any details that could lead to the access control system being defeated by an adversary, external or internal, should not be released.
1.8. Stores: Security procedures for the issue, receipt and control of material stock; names of authorized key holders; arrangements for monitoring and guarding	N, R	Sensitive	Of potential use to adversaries planning malicious acts.
1.9. General maps showing the position and limits of a facility but without detail of what is contained within	N, R	Not sensitive	Freely available Internet mapping applications show such information clearly.
1.10. Other physical protection associated matters, e.g. location, set-up, manning and equipment at the central alarm station; location of the secondary alarm station; type of inner area barrier	N, R	Sensitive	Any details of this nature would be of great use to any adversary who wished to defeat the security systems at nuclear facilities.
2. INFORMATION RELATING TO THE QUANTITY AND FORM OF MATERIAL			
2.1. Information about the quantity, type and form of nuclear material, including sources, received or held in specified locations on all categories of site and nuclear power plant, including the exact locations where spent fuel is held	N	Sensitive	The type of information could be of use to adversaries choosing targets while planning attacks.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
2.2. Throughput — nominal capacity, actual throughput and historical data on throughput of a facility under IAEA safeguards	N	Not sensitive	Such high level information, especially for nuclear power plants, is often in the public domain.
2.3. Inventories, either national or local, of other radioactive material (including disused material), including the quantity, type, form and exact location	R	Sensitive	This type of information could be of use to adversaries choosing targets while planning attacks in order to steal radioactive material. Consideration should be given on which information is already publicly available with regard to such inventories. All such information may not be considered sensitive. Risk informed processes will help determine whether something should be designated as sensitive.
3. MATERIAL IN TRANSIT (INCLUDING MOVEMENT WITHIN A SITE)			
3.1. Information on Category I, II, III movements of nuclear material	N	Sensitive	Such information could aid in choosing targets while planning malicious acts involving nuclear material in transit.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
3.2. High security vehicles (HSVs)			
A. Visual access to interior of cab and cargo compartment	N	Sensitive	HSVs are vehicles specially designed to transport nuclear material securely. HSVs carry nuclear material and any information of the type listed in this section could be of use to an adversary planning an attempt to steal or sabotage nuclear material in transit.
B. Physical security features of vehicle design and construction	N	Sensitive	
C. Design and function of alarms, immobilization devices and key designs for special locks	N	Sensitive	
D. Load compartment keys, spare keys and combination lock settings, where used	N	Sensitive	
E. Vehicle tracking system if fitted to the HSV; system performance and communications	N	Sensitive	
3.3. Nuclear material transit containers			
A. Level of resistance of transport containers to attack by various means	N	Sensitive	Useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport.
B. Specifications and design data on containers	N	Not sensitive	Information on the design of such containers without identification of construction details is often available on the Internet.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
C. Information on the design of specific containers (specially protected containers)	N	Sensitive	Useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport.
3.4. Transport packages: Information on the design of transport packages	N	Sensitive	Useful to an adversary planning a sabotage attack with the aim of releasing nuclear material or planning the theft of the material during transport.
3.5. Information on movements of other radioactive material	R	Sensitive	This type of information, particularly if concerned with the transport of powerful radiation sources, could be of use in planning a theft.
4. IT SYSTEMS AND COMPUTER SYSTEMS IMPORTANT TO SECURITY AND SAFETY			
4.1. Details of IT systems storing and processing sensitive information, including the systems used for security purposes, system architecture, details of computer security measures employed and location of backup media	N, R	Sensitive	Information useful to an adversary planning a malicious act at a facility.
4.2. Details of access control, intrusion detection systems, alarm monitoring systems, assessment and surveillance systems and other security functions and devices; and information on the location of backup hardware and software	N, R	Sensitive	Information useful to an adversary planning a malicious act at a facility.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
4.3. Details of safety related IT systems or computer systems important to safety, including the locations, functions, upgrade routes, power supply and backup	N, R	Sensitive	Such systems have control and operational monitoring functions. Successful compromise of these systems could enable an adversary, at the least, to disrupt the operation of a facility, and in the worst case disruption could lead to a radioactive release.
5. GUARD FORCES AND RESPONSE FORCES			
5.1. Guard force at a facility			
A. Overall establishment and the current capabilities of the force	N	Not sensitive	Publicizing the existence of a force can reassure the public and potentially act as a deterrent.
B. Establishment and current capabilities at particular sites	N	Sensitive	Information of this nature could be of use to any adversary in planning an incursion into a nuclear site for the purpose of sabotage or theft and could undermine the capability for effective response to an attack.
C. Numbers on any shift at a site	N	Sensitive	

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
D. Weapons and other special equipment available to the guard force and the number of trained users of firearms in the guard force individual sites	N	Sensitive	Any information that could help an adversary to estimate in advance the scale of response and the capabilities available in a tactical operational unit should be secured against disclosure.
E. Response force location, capabilities, weapons, special response vehicles and timings at a site	N	Sensitive	
F. Deployment plans	N	Sensitive	
5.2. Escorts for nuclear material movements			
A. Deployment and capabilities of the escort	N	Sensitive	
B. Radio frequencies in use to enable communication with a response force or local police forces	N	Sensitive	Information could be of use to an adversary planning to attack a convoy.
6. NUCLEAR MATERIAL ACCOUNTING			
6.1. Description			
A. Statements of general material accounting principles	N	Not sensitive	General principles of this type exist in the public domain.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
B. Design information questionnaire and description, and location of material balance areas (MBAs) and key measurement points (KMPs)	N	Sensitive	Such detailed information on the location and quantities of nuclear material could be of use to an adversary planning a malicious act.
C. Physical and chemical form of material measurement at KMP	N	Sensitive	
6.2. Measurements and instrumentation data			
A. Precision and accuracy of standard laboratory techniques	N	Not sensitive	This information is often in the public domain.
B. Data which reveal the sensitivity of measurement or the alarm limits for material unaccounted for (MUF) at a particular plant	N	Sensitive	Precision and accuracy data relating to actual or typical measurements at sites, whether aggregated or disaggregated, could be of use to an adversary planning theft of material.
6.3. Nuclear material flow and inventory data held on IT systems, in hard copy or on any form of storage medium	N	Sensitive	Information could reveal exact details of the location and movements of nuclear material.
6.4. Material unaccounted for			
A. Annual MUF figures for a site which does not reveal the MBA concerned	N	Not sensitive	In many States, aggregated annual MUF figures are, or can be, published in the public domain.
B. MUF in MBAs or KMPs	N	Sensitive	

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
C. Details of investigations into particular MUF unless formally approved for release	N	Sensitive	However, detailed MUF figures or investigation results could be of use to an adversary in targeting a specific facility and therefore should be considered sensitive.
D. Limit of error for MUF or other specific indications of the uncertainty of MUF figures	N	Sensitive[a]	
7. LICENSING AND PERMISSIONS PROCESS APPLICATIONS			
7.1. Licensing and permissions process applications without detailed information on security measures; type, form and quantity of material	N, R	Not sensitive	Content of such an application will vary depending on the legal and regulatory framework and the specific end use. If applications contain sensitive information that could be of potential use to an adversary, the application should also be treated as sensitive information.
7.2. Licensing and permissions process applications containing detailed information on, e.g., security measures, and type, form and quantity of material	N, R	Sensitive	Content of such an application will vary depending on the legal and regulatory framework and the specific end use. If applications contain sensitive information that could be of potential use to an adversary, the application should also be treated as sensitive information.
8. SAFETY CASES, ENGINEERING DOCUMENTS AND OTHER SAFETY OR ENVIRONMENTAL INFORMATION			
8.1. Safety cases of all classes			While most information with regard to safety cases may be made public for transparency, some information may be considered sensitive with regard to nuclear security.

[a] In some States, the limit of error for MUF is not considered to be sensitive information.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
A. Details of the potential hazards or other information that could be used as a surrogate for evaluating the impact of a release, or details on the impacts of releases	N, R	Sensitive	
B. Details of strengths and weaknesses of processes, structures and protection systems designed to contain, control or secure nuclear material or other radioactive material	N, R	Sensitive	The type of detailed information contained in safety cases could be of use to an adversary for choosing targets and planning an operation.
C. Details of access to the production process, both physical access control and the removal of material from the process for control and monitoring purposes	N, R	Sensitive	
9. CONTINGENCY AND RESPONSE PLANS AND EXERCISES			
9.1. Contingency and response			
A. Existence of a contingency and response plan	N, R	Not sensitive	Publicizing the existence of plans can reassure the public and potentially act as a deterrent.
B. Detailed contents of a contingency and response plan	N, R	Sensitive	Details from the plan could indicate the capabilities, limitations and response times, and therefore be of use to an adversary in planning a deliberate attack.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
9.2. Security contingency plans, including detailed information	N, R	Sensitive	Such documents contain information on the security measures in place, on the capabilities of the police or guard force contingents and on the likely response to a security incident.
9.3. Exercises			
A. That an exercise is to take or has taken place	N, R	Not sensitive	Publicizing the existence of exercises can reassure the public, provided that the level of detail would not assist an adversary, e.g. date/time/location of a future exercise.
B. Details of security exercises at a site including the scenario, which aspects of the security plan are being tested, whether a response force will be involved and the results of the exercise	N, R	Sensitive	Provides adversaries with information on the nature, size, capabilities and timing of response force reaction, detail of armed response force, nature of tactics employed and signal plan.
C. Details of safety exercises	N, R	Not sensitive	Safety exercises are often run in an open and transparent manner. They can typically be considered non-sensitive as long as they do not reveal detailed information on security measures.
10. PERSONAL INFORMATION			
10.1. Personal information			
A. Information from trustworthiness checks	N, R	Sensitive	Information of this nature could be used for blackmail or extortion. Most national privacy regulations will mandate the protection of this type of information.
B. Information in personnel files	N, R	Sensitive	

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
11. RADIOACTIVE WASTE INVENTORY			
11.1. Information on radioactive waste			
A. General information about inventories that does not contain any information that could be exploited, e.g. the fact that waste is stored at a particular site, or aggregated quantities of waste without location	N	Not sensitive	Such information is generally in the public domain and does not describe specifics of use to an adversary.
B. Information that could be used in a malicious act or enables a specific building at a facility and the material held there to be identified	N	Sensitive	Such information provides targeting information for an adversary planning sabotage.
12. DECOMMISSIONING			
12.1. Plans to decommission plant	N, R	Not sensitive	Plans to decommission facilities are often publicly announced.
12.2. Waste from decommissioning[b]			
A. That a store is to be built, and its location.	N, R	Not sensitive	This information is often in the public domain.

[b] This refers mainly to contaminated materials from the facility, rather than radioactive waste from the processes conducted during normal operation of the facility.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
B. Detail of the construction, security measures and quantity or type of material to be stored in new builds for the treatment and storage of waste and contaminated material arising from processing activities during decommissioning	N, R	Sensitive	This information can provide useful targeting information for an adversary planning sabotage attacks.
13. THREAT ASSESSMENTS AND SECURITY ALERTING INFORMATION			
13.1. Threat assessments issued by the State, national security authorities or other competent authorities	N, R	Sensitive	Typically derived from national security material, e.g. national intelligence information.
13.2. Details of the design basis threat	N	Sensitive	Typically derived from national security material, e.g. national intelligence information.
13.3. Details of the vital area identification study	N	Sensitive	Could be of use to an adversary in identifying targets and carrying out an attack.
13.4. Reasons for any security alert state in place and for any changes to it	N, R	Sensitive	Typically derived from national security material, e.g. national intelligence information.
14. NUCLEAR TECHNOLOGY			
14.1. Detailed technical information about the production or processing of nuclear material (e.g. enriched uranium processing and reprocessing)	N	Sensitive	Information of this type could be of use to an adversary.

TABLE II–1. NOTIONAL SECURITY CATEGORIZATION SCHEME FOR NUCLEAR SECURITY RELATED INFORMATION (cont.)

Category	Area	Sensitivity	Rationale for securing
14.2. Designs or new technology submitted for licensing (e.g. advanced reactor technology, etc.)	N	Sensitive	Although details of these technologies may be made available to the public, it is possible that some detail of the design or technology could be of use to adversaries for planning purposes. Such information may be reviewed for sensitive information.
14.3. Detailed information that would assist in disassembly of devices to gain access to sources or would otherwise assist in defeating security measures	R	Sensitive	This information could be of use to an adversary attempting to remove radioactive material.
14.4. Vulnerability studies of technology designs	N, R	Sensitive	Although academic studies may be publicly available, any detailed information exposing vulnerabilities that could be exploited by an adversary should be secured against unauthorized disclosure.
15. HISTORICAL INFORMATION			
15.1. Historical information of current relevance and still sensitive, whether or not the information is classified	N, R	Sensitive	Information of this nature, although old, may still be of use to adversaries.

Note: HSV — high security vehicle; KMP — key measurement point; MBA — material balance area; MUF — material unaccounted for; N — nuclear material and nuclear facilities; R — other radioactive material and associated facilities.

Annex III

SAMPLE SECURITY AWARENESS PROGRAMME

III–1. Annex III provides an example framework and content for establishing a security awareness programme. When deciding the content of an information security awareness programme, an organization's security manager should consider the specific relevance of the topics and methods highlighted here and adapt the programme accordingly.

SECURITY TRAINING

III–2. Training can be broadly divided into four types:

(a) Awareness training increases awareness of threats and vulnerabilities and recognition of the need to protect data, information and the means of processing them (computer and information security awareness).
(b) Topical training includes courses on specific aspects of security for all staff (classified material handling and information security incident procedures).
(c) Professional training is typically detailed technical training for staff with particular responsibilities, for example for system administrators, software developers, network administrators, security guards, document classifiers and declassifiers, among others.
(d) Specialized security training is focused and expert level training, usually for management level, in the areas of risk management, incident prevention and incident response, among other things.

III–3. The programme could include content to raise awareness on the following topics:

(a) Overview of the national security infrastructure.
(b) Aspects of information security and why they are important to nuclear security.
(c) The national classification system.
(d) Security principles, for example 'need to know' and 'need to hold'.
(e) Current threats to security arising from deliberate actions by:
    (i) Hostile intelligence services in respect of espionage and technology transfer;
    (ii) Subversive organizations;

(iii) Other individuals and groups, such as information brokers and investigative journalists seeking to gain unauthorized access to sensitive information or nuclear sites and facilities;

(iv) Insiders.

(f) The threat from adversary organizations and from sabotage, taking account of the contemporary world threat from any extremist factions.

(g) The risks and consequences of internal loss or leaks of sensitive information, perhaps through inadvertent behaviour or to cause embarrassment, together with deliberate betrayal for political motives or to assist terrorism.

(h) Conduct or activities likely to help potential adversaries or increase the risk of compromise, including:

(i) Vulnerable behaviour such as casual attitudes to security and loose talk;

(ii) Unwitting behaviour that can attract the attention of hostile agencies and precautions needed in everyday activities, including, for example, social approaches, travel, correspondence and acquaintances.

(i) Information on topical security events or new types of approach being used by hostile agencies, which should be disseminated rapidly.

(j) Emphasis on the need to report immediately all suspicious circumstances, perceived weaknesses in security procedures or vulnerable behaviour apparent in colleagues — the means of doing this in confidence should be widely briefed.

(k) The effect of national laws and regulations and their relevance to individuals, for example, laws governing secrecy, anti-terrorism, security, data protection and freedom of information, and the sanctions and the punishment for transgression.

(l) Explain the levels of security clearances; how trustworthiness checks are carried out; why they are necessary in the nuclear and radiological industry; and which levels of access relate to particular clearance and trustworthiness levels — in addition, how this relates to the threats to security mentioned above.

(m) Denial of service (e.g. preventing an organization from having access to the information when needed, including actions such as theft) or destruction — a breach of availability.

(n) Unauthorized modification of or interference with information — a breach of integrity.

(o) Unauthorized disclosure — a breach of confidentiality.

III–4. The programme could include content to train participants on the following topics:

(a) The security of information regarding nuclear material and other radioactive material and facilities.
(b) Good security practice and procedure including:
  (i) Correct use of classification markings;
  (ii) Physical protection, personnel security and information security (e.g. documents, communications and computers);
  (iii) Practical examples of applying the security rules and procedures in the tasks in which employees are, or will be, engaged;
  (iv) Actions to be taken if a breach of security is suspected or discovered.

ADDITIONAL METHODS OF PROMOTING SECURITY

III–5. In addition to a fundamental training programme, there are a number of other methods by which security awareness messages can be brought to the attention of employees and contractors:

(a) Regular security newsletters published by the national security authorities. These can contain issues of topical interest and advice on a range of security matters.
(b) Posters to remind individuals of the threats to security and of the principal security controls necessary to counter them. Their impact tends to be temporary, so posters should not only be prominently displayed but also frequently changed.
(c) Stickers to remind employees of their personal responsibility for the maintenance of security when using specific items of equipment.
(d) Security reminder notices in the startup (boot) phase of a computer system, which the user has to acknowledge reading before the computer will finish booting or logging in. (Systems can record such acknowledgements so that a user cannot deny having seen the notice.)
(e) Security notices, bulletins and circulars drafted by security management to remind staff of certain security rules, to counter possible complacency, among other things.
(f) Raising awareness of instances of breaches of security and the lessons to be learned from them.
(g) Warning individuals of specific or topical threats to security and providing guidance to counter them.

(h) Providing a channel of communication with individuals on security matters generally.

(i) Regular periodic tests of individual security knowledge.

(j) An organization's intranet can also be a valuable tool in conveying or promoting the security message so long as the nature and sensitivity of the material remain within the accredited level of classification for the network.

GLOSSARY

availability. The property of being accessible and usable upon demand by an authorized entity.

competent authority. A governmental organization or institution that has been designated by a State to conduct one or more nuclear security functions.

compromise. The accidental or deliberate violation of confidentiality, loss of integrity or loss of availability of an information object.

confidentiality. The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

information object. Knowledge or data that have value to the organization.

information security. The preservation of the confidentiality, integrity and availability of information.

integrity. The property of accuracy and completeness of information.

need to hold. Rule by which individuals are permitted to have in their physical possession only the information assets that are necessary to conduct their work effectively.

need to know. Rule by which individuals, processes and systems are granted access to only the information, capabilities and assets that are necessary for execution of their authorized functions.

nuclear material. Any material that is either special fissionable material or source material as defined in Article XX of the IAEA Statute.

other radioactive material. Any radioactive material that is not nuclear material.

radioactive material. Any material designated in national law, regulation or by a regulatory body as being subject to regulatory control because of its radioactivity.

sensitive information. Information, in whatever form, including software, the unauthorized disclosure, modification, alteration, destruction, or denial of use of which could compromise nuclear security.

sensitive information assets. Any equipment or components that are used to store, process, control or transmit sensitive information. For example, sensitive information assets include control systems, networks, information systems and any other electronic or physical media.

IAEA
International Atomic Energy Agency

No. 23

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

AUSTRALIA
DA Information Services
648 Whitehorse Road, Mitcham, VIC 3132, AUSTRALIA
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: books@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
5369 Canotek Road, Ottawa, ON K1J 9J3, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, spol. S.r.o.
Klecakova 347, 180 21 Prague 9, CZECH REPUBLIC
Telephone: +420 242 459 202 • Fax: +420 242 459 203
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa
PO Box 128 (Keskuskatu 1), 00101 Helsinki, FINLAND
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

FRANCE
Form-Edit
5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 50 80 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 8740 • Fax: +49 (0) 211 49 87428
Email: s.dehaan@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotrade Ltd., Book Import
PF 126, 1656 Budapest, HUNGARY
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 2261 7926/27 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: http://www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: http://www.libreriaaeiou.eu

JAPAN

Maruzen Co., Ltd.

1-9-18 Kaigan, Minato-ku, Tokyo 105-0022, JAPAN
Telephone: +81 3 6367 6047 • Fax: +81 3 6367 6160
Email: journal@maruzen.co.jp • Web site: http://maruzen.co.jp

NETHERLANDS

Martinus Nijhoff International

Koraalrood 50, Postbus 1853, 2700 CZ Zoetermeer, NETHERLANDS
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

SLOVENIA

Cankarjeva Zalozba dd

Kopitarjeva 2, 1515 Ljubljana, SLOVENIA
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.mladinska.com/cankarjeva_zalozba

SPAIN

Diaz de Santos, S.A.

Librerias Bookshop • Departamento de pedidos
Calle Albasanz 2, esquina Hermanos Garcia Noblejas 21, 28037 Madrid, SPAIN
Telephone: +34 917 43 48 90 • Fax: +34 917 43 4023
Email: compras@diazdesantos.es • Web site: http://www.diazdesantos.es

UNITED KINGDOM

The Stationery Office Ltd. (TSO)

PO Box 29, Norwich, Norfolk, NR3 1PD, UNITED KINGDOM
Telephone: +44 870 600 5552
Email (orders): books.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

UNITED STATES OF AMERICA

Bernan Associates

4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.

812 Proctor Avenue, Ogdensburg, NY 13669, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

United Nations

300 East 42nd Street, IN-919J, New York, NY 1001, USA
Telephone: +1 212 963 8302 • Fax: 1 212 963 3489
Email: publications@un.org • Web site: http://www.unp.un.org

Orders for both priced and unpriced publications may be addressed directly to:

IAEA Publishing Section, Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22488 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

14-51841

OBJECTIVE AND ESSENTIAL ELEMENTS OF A STATE'S NUCLEAR SECURITY REGIME
IAEA Nuclear Security Series No. 20
STI/PUB/1590 (15 pp.; 2013)
ISBN 978–92–0–137810–1
Price: €20.00

NUCLEAR SECURITY RECOMMENDATIONS ON NUCLEAR AND OTHER RADIOACTIVE MATERIAL OUT OF REGULATORY CONTROL
IAEA Nuclear Security Series No. 15
STI/PUB/1488 (33 pp.; 2011)
ISBN 978–92–0–112210–0
Price: €23.00

NUCLEAR SECURITY RECOMMENDATIONS ON RADIOACTIVE MATERIAL AND ASSOCIATED FACILITIES
IAEA Nuclear Security Series No. 14
STI/PUB/1487 (27 pp.; 2011)
ISBN 978–92–0–112110–3
Price: €22.00

NUCLEAR SECURITY RECOMMENDATIONS ON PHYSICAL PROTECTION OF NUCLEAR MATERIAL AND NUCLEAR FACILITIES (INFCIRC/225/REVISION 5)
IAEA Nuclear Security Series No. 13
STI/PUB/1481 (57 pp.; 2011)
ISBN 978–92–0–111110–4
Price: €28.00

The security of sensitive information in nuclear security is a fundamental principle. Sensitive information is information, the unauthorized disclosure (or modification, alteration, destruction or denial of use) of which could compromise nuclear security or otherwise assist in the carrying out of a malicious act against a nuclear facility, organization or transport. This Implementing Guide defines the basic concepts of information security as it might apply to nuclear security to help Member States and organizations with nuclear security responsibilities to develop a framework of information security.

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–110614–8
ISSN 1816–9317